REMARKS

Applicant previously argued on Appeal that the proposed combination of U.S. Patent Number 5,940,508 ("Long") in view of U.S. Patent Number 5,081,679 ("Dent") fails to describe or suggest a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system including, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

The Examiner disagrees and, in response, asserts that Dent "teaches producing new keystream bits (generating new key) when there is handoff (the handoff is due to a change of component in transmitting the voice packets. . .) that meets the recitation of when a component used to transmit the Real Time Protocol voice packets changes, generate a second key." Office Action at page 3. Applicant disagrees. The handoff refers to a "process of switching an established call from one cell to another." Dent at col. 4, lines 26-28. As such, to the extent a second key is generated, the generation thereof is between the mobile device and a new base station to which the traffic is transferred, and not between the original base station and the mobile device. In contrast, in one aspect, the instant application describes generating the first key and the second key between a local multimedia terminal adapter and a remote multimedia terminal adapter and not between the local multimedia terminal adapter and two different remotes multimedia terminal adapters.

Accordingly, Dent fails to describe or suggest a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system including, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

Notwithstanding the above and as pointed out in Applicant's appeal, Dent cannot be combined with Long because Long expressly teaches away from the teachings of Dent. In response, the Office Action asserts that "[t]he prior art mere disclosure of conventional art does not constitute a teaching away because such disclosure does not discredit the conventional art but rather offers a balance depending on design choices." Office Action at page 3. This argument, however, fails to address the fact that Dent teaches a system that requires suspension of data traffics (e.g., voice data) to enable resynchronization (e.g., changing the block counter of mobile device). *See e.g.*, Dent at Abstract, at col. 6, lines 41-58 and col. 14, lines 21-49. In Long's view such a system has several disadvantages.

In particular, Long describes that in Dent's system the need for resynchronization can cause downtime on the link and can result in a loss or blockage of huge amount of data. Long at col. 1, lines 28-37. Furthermore, Long describes that the data can be real-time data, where the loss of data is not protected through buffering or protocols. Long at col. 1, lines 38-39. Because of these disadvantages, Long teaches away from the system of Dent and describes a system that seamlessly performs resynchronization, thereby eliminating the downtime associated with Dent's system. *See e.g.*, Long at col. 1, line 65 to col. 2, line 3. That is, Long teaches away from Dent's system by advocating a system that seamlessly updates the resynchronization information instead of halting traffic between the encryptor and the decryptor equipments. *See e.g.*, Long at col. 2, lines 21-28.

For at least the foregoing reasons, Applicant continues to assert that the proposed combination of Long and Dent fails to describe or suggest the above-recited features of claim 1.

Although the Office Action fails to concede to these points, it nevertheless relies on a new reference to remedy these shortcomings. In particular, the Office Action now relies on U.S. Patent Application Publication Number 2002/0006202 ("Fruehauf") to show the above-recited feature of claim 1 as described in detail below.

Specification

The specification was objected to as allegedly failing to provide proper antecedent basis for "a component used to transmit the Real Time Protocol voice packets changes during the communication session." Applicant respectfully submits, at a minimum, originally filed claims 2 and 3 provide support for this feature. Accordingly, Applicant respectfully requests reconsideration and withdrawal of this objection.

Claim Rejections – 35 U.S.C. § 112

Claims 17-18 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. Applicant has amended claim 17 to overcome this rejection. Accordingly, Applicant respectfully requests reconsideration and withdrawal of this rejection.

Claim Rejections – 35 U.S.C. § 103

Claims 1-3, 6, 7, 10-16, and 19-23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Long in view of Fruehauf and further in view of Dent. Applicant disagrees because Long, Fruehauf, and Dent, either alone or in combination, fail to describe or suggest a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system including, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

The Office Action asserts Fruehauf provides such teachings. Fruehauf relates to a system and a method for secure cryptographic communications. Fruehauf at Title. Referring to FIG. 1 of Fruehauf, the system includes a data encryptor (107) and three data decryptors (112-114). Fruehauf at page 3, paragraph 35. Each of the data encryptor (107) and data decryptors (112-114) obtain a key from key storage units (104) and (117), respectively. *Id.* The key storage units (104) and (117) generates key *based on the **time** data in clocks (103) and (116). Id.* As such, similar to Long, Fruehauf also describes a system in which the keys are generated based on ***time*** and assigned to the encryptor (107) and data decryptors (112-114).

To illustrate further, Fruehauf describes

> **During the encryption process, unencrypted data 106 ("red data") is input to the data encryptor 107. The data encryptor 107 holds a key obtained from the key storage unit 104 and encrypts the red data 106 with the key during the key period. For example, referring to FIG. 1A, the consecutive use of three different keys, keys A, B, and C is illustrated. If the key period is set to be one minute, and if the clock 103 is at a time of about 8:01 AM, then the data encryptor 107 obtains a key B from the key storage unit 104 and holds key B for one minute. During this one minute, if the red data 106 is input to the data encryptor 107, then the data encryptor 107 encrypts the red data 106 with key B. However, in the present example, if the time on the Clock 103 is showing 8:02 AM, then the data encryptor 107 obtains key C from the key storage unit 104 and then encrypts with key C the inputted data. Note that for the purposes of explaining the present invention, arbitrary times of 8:00 AM, 8:01 AM, and 8:02 AM have been selected with a key period of one minute. As previously mentioned, the key period can be any length of time.**
>
> **In FIG. 1, the encrypted data ("black data") passes through protocols 108 and is then released into the communications media or channel 110 for delivery to the intended receiver. The black data is received and preferably passes through the applicable protocols 111 and is received by all three data decryptors 112-114 preferably at about the same time. In the present example, since the clock 116 is showing 8:01 AM, the data decryptor 113 is expected to decrypt the black data since the data decryptor 113 is synchronized to the current key period showing on the clock 116. The current key period ranges from approximately 8:01:00 AM to approximately 8:01:59 AM. The data**

> **decryptor 112 is synchronized to the preceding key period of the clock 116, which in the present example ranges from approximately 8:00:00 AM to approximately 8:00:59 AM. The data decryptor 114 is synchronized to the succeeding key period of the clock 116, which in the present example ranges from approximately 8:02:00 AM to approximately 8:02:59 AM.**

Fruehauf at page 3, paragraphs 37, 38. Accordingly, Fruehauf also fails to describe or suggest a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network, the system including, among other features, a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1. For example, Fruehauf does not describe or otherwise suggest generating a second key stream when a first coder/decoder for compressing/decompressing the voice packets changes to a second coder/decoder, as recited in claim 2. For another example, Fruehauf does not describe or otherwise suggest generating a second key stream when a Message Authentication Code algorithm changes, as recited in claim 3.

The Office Action asserts that Fruehauf describes this feature on page 4, paragraph 42. Applicant disagrees. On page 4, paragraph 42, Fruehauf merely describes "only one of the three parallel decryptors (112-114), for instance decryptor (113), is expected to be decrypting the data at any given time; when a transition from one data decryptor to another data decryptor occurs it means that the data decryptors (112, 113, and 114) have changed keys. . ." This, without more, does not describe or suggest a local key stream generator and a remote key stream generator generating a second key stream *when a component used to transmit the Real Time Protocol voice packets changes* during the communication session and a packet encryptor and a packet decryptor use the second key stream, as recited in claim 1.

For at least the foregoing reasons, Applicant respectfully request reconsideration and withdrawal of the rejection of claim 1, along with its dependent claims.

Claim 6 recites a system for communicating Real Time Protocol voice packets between a local and a remote location over an Internet protocol network. The system includes, among other features, a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system switches from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the synchronization of the key stream, wherein the first communication parameter is a first coder/decoder that compresses/decompresses the voice packets, and the second communication parameter is a second coder/decoder that compresses/decompresses the voice packets. Therefore, for at least the reasons presented above with respect to claim 1, Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 6, along with its dependent claims.

Claim 19 recites a system for securely transmitting voice packets during a communication session from a local location to a remote location over a communication network. The system includes, among other features, a means for decrypting the encrypted voice packets using the first key stream and a means for generating the first key stream at the remote location in order to decrypt the encrypted voice packets, wherein both means for generating are capable of generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session. Therefore, for at least the reasons presented above with respect to claim 1, Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 19, along with its dependent claims.

Claims 17 and 18 were rejected as being unpatentable under 35 U.S.C. § 103(a) over Long, in view of Dent, and further in view of Crichton. Applicant respectfully traverses this rejection because the proposed combinations of Long, Dent, and Crichton fails to describe or suggest a method for securely transmitting Real Time Protocol voice packets from a local location to a remote location, the method including, among other steps, a step of generating a second Real Time Protocol key stream for encrypting the voice packets during a communication session in response to ***a collision detection***.

The Office Action concedes that Long fails to describe this feature. However, the Office Action asserts that Dent provides such teaching. In particular, the Office Action asserts that "Dent discloses a collision is detected wherein the multimedia terminal adapters have the same source identifier (see column 14, lines 21-49) and further discloses generating a second stream in response to handoff as discussed above with respect to claim 1 (see also column 15, lines 30-44)." However, as noted above with respect to claim 1, the handoff refers to a "process of switching an established call from one cell to another." Dent at col. 4, lines 26-28. As such, to the extent a second key is generated, the generation thereof is between the mobile device and a new base station to which the traffic is transferred, and not between the original base station and the mobile device.

In contrast, in one aspect, the instant application describes generating the first key and the second key between a local location and a remote location and not between a local location and two remote locations.

Crichton was cited for an alleged showing of a gateway. As such, Applicant does not believe that the proposed addition of the subject matter from Dent and Crichton remedy the shortcomings of Long and Dent to describe or suggest the above-recited features of claim 17.

For at least the foregoing reasons, Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 17, along with its dependent claim.

Based on the foregoing, it is respectfully submitted that all pending claims are patentable over the cited prior art. Accordingly, it is respectfully requested that the rejections under 35 U.S.C. § 103 be withdrawn.

Conclusion

Having fully responded to all matters raised in the Office Action, Applicant submits that all claims are in condition for allowance, an indication for which is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicant's attorney at the telephone number shown below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP

Michael E. Fogarty
Registration No. 36,139

**Please recognize our Customer No. 20277
as our correspondence address.**

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 BA:MaM
Facsimile: 202.756.8087
Date: April 3, 2009